#2

THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re the Application of : **Makoto KUBOTA, et al.**

Filed : **Concurrently herewith**

For : **COMMUNICATION DATA RELAY SYSTEM....**

Serial No. : **Concurrently herewith**

March 21, 2001

Assistant Commissioner of Patents
Washington, D.C. 20231

SUBMISSION OF PRIORITY DOCUMENT

S I R:

Attached herewith are Japanese patent application No. 2000-102701 of April 4, 2000 whose priority has been claimed in the present application.

Respectfully submitted

[ ]Samson Helfgott
Reg. No. 23,072
[x]Aaron B. Karas
Reg. No. 18,923

HELFGOTT & KARAS, P.C.
60th FLOOR
EMPIRE STATE BUILDING
NEW YORK, NY 10118
DOCKET NO.:FUJY 18.457
BHU:priority

Filed Via Express Mail
Rec. No.: EL522402424US
On: March 21, 2001
By: Brendy Lynn Belony
Any fee due as a result of this paper, not covered by an enclosed check may be charged on Deposit Acct. No. 08-1634.

01/1143

J1040 U.S. PTO
09/814235
03/21/01

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。
This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２０００年 ４月 ４日

出願番号
Application Number: 特願２０００－１０２７０１

願人
Applicant (s): 富士通株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

２０００年１２月１５日

特許庁長官
Commissioner,
Patent Office 及川耕造

出証番号 出証特２０００－３１０４６９９

【書類名】　特許願
【整理番号】　9951378
【提出日】　平成12年 4月 4日
【あて先】　特許庁長官殿
【国際特許分類】　H04L 12/22
H04L 12/24
【発明の名称】　通信データ中継装置、及び方法
【請求項の数】　7
【発明者】
【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
【氏名】　久保田　真
【発明者】
【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
【氏名】　小口　直樹
【発明者】
【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
【氏名】　鶴岡　哲明
【特許出願人】
【識別番号】　000005223
【氏名又は名称】　富士通株式会社
【代理人】
【識別番号】　100089244
【弁理士】
【氏名又は名称】　遠山　勉
【選任した代理人】
【識別番号】　100090516

【弁理士】

【氏名又は名称】　松倉　秀実

【連絡先】　０３－３６６９－６５７１

【手数料の表示】

【予納台帳番号】　012092

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9705606

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　通信データ中継装置、及び方法

【特許請求の範囲】

【請求項１】１以上の通信装置を接続した、そのような２以上のネットワーク間を中継する通信データ中継装置であって、

前記ネットワークにアクセスするための２以上のインターフェース部と、

１以上のネットワークを接続したシステムとしてのドメインを定義するドメイン定義部と、

２以上のドメイン間における接続の可否を定義するドメイン間接続定義部と、

通信データの中継先を記憶する経路情報記憶部と、

異なるドメイン間で通信データを中継するときに、送信側ドメインにおける送信元アドレスと中継先ドメインにおける送信元アドレスとを相互に変換するアドレス変換部と、

前記ドメイン間接続定義部の定義に従い２以上のドメイン間における中継の可否を制御する制御部とを備えた通信データ中継装置。

【請求項２】１以上の通信装置を接続した、そのような２以上のネットワークを中継する通信データ中継装置であって、

前記ネットワークにアクセスするための２以上のインターフェース部と、

１以上のネットワークを接続したシステムとしてのドメインを定義するドメイン定義部と、

２以上のドメイン間における接続の可否を定義するドメイン間接続定義部と、

通信データの中継先を記憶する経路情報記憶部と、

異なるドメイン間で通信データを中継するときに、送信側ドメインにおける送信先アドレスと中継先ドメインにおける送信先アドレスとを相互に変換するアドレス変換部と、

前記ドメイン間接続定義部の定義に従い２以上のドメイン間における中継の可否を制御する制御部とを備えた通信データ中継装置。

【請求項３】前記ドメイン定義部は、ドメインを、そのドメインに接続されるインターフェース部を識別する情報によって定義する請求項１または２のいずれ

かに記載の通信データ中継装置。

【請求項４】前記制御部は、通信データを受信したインターフェース部に対応付けられるドメイン（または通信データを受信したインターフェース部）と、

その通信データの送信元アドレスが属するドメイン（またはその通信データの送信元アドレスが属するドメインに対応付けられるインターフェース部）とが、異なる通信データを廃棄する請求項１または２のいずれかに記載の中継装置。

【請求項５】前記ドメイン定義部は、各ドメインごとに、そのドメインに含まれるネットワークを識別するアドレス（またはそのドメインに含まれるネットワークに接続される通信装置を識別するアドレス）によって定義される請求項１または２のいずれか記載の通信データ中継装置。

【請求項６】各々１以上の通信装置に接続された、そのような２以上のネットワークを中継する通信データ中継方法であって、

１以上のネットワークを接続したシステムとしてのドメインを定義するドメイン定義部を検索する手順と、

２以上のドメイン間における接続の可否を定義するドメイン間接続定義部を検索する手順と、

通信データの中継先を記憶する経路情報記憶部を検索する手順と、

異なるドメインで通信データを中継するときに、送信側ドメインにおける送信元アドレスと中継先ドメインにおける送信元アドレスとを相互にアドレス変換する手順とを備え、

前記ドメイン間接続定義部の検索結果に従い２以上のドメイン間における中継の可否を制御する通信データ中継方法。

【請求項７】各々１以上の通信装置に接続された、そのような２以上のネットワークを中継する通信データ中継方法であって、

１以上のネットワークを接続したシステムとしてのドメインを定義するドメイン定義部を検索する手順と、

２以上のドメイン間における接続の可否を定義するドメイン間接続定義部を検索する手順と、

通信データの中継先を記憶する経路情報記憶部を検索する手順と、

異なるドメイン間で通信データを中継するときに、送信側ドメインにおける送信先アドレスと中継先ドメインにおける送信先アドレスとを相互にアドレス変換する手順とを備え、

前記ドメイン間接続定義部の検索結果に従い２以上のドメイン間における中継の可否を制御する通信データ中継方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明はパケットの中継装置に関わり、特に、異なるパケットルーティング規則を持つため、直接パケットが到達できない通信ネットワーク同士の接続機能、アドレス変換機能に関する。

【０００２】

【従来の技術】

（ドメインの概念）

従来、ネットワーク層において、ドメインは以下のように定義されている。

［ドメイン］

ドメインとは、ネットワーク層において共通の経路制御ルールに従いパケットを送信可能な範囲である。なお、異なる経路制御ルールを用いたエリア同士間では、中継装置を介さなければパケットは到達できない。

【０００３】

以下はそれぞれ異なるドメインの例である。

企業内網とインターネット：企業内網ではInterior Gateway Protocol(IGP)を用いた独自の経路制御が行われ、インターネットではExterior Gateway Protocol(EGP)を用いた経路制御が行われる。一般的には企業内網の経路情報はインターネットに配布されない。

【０００４】

IPv4ネットワークとIPv6ネットワーク：これらは共通の通信メディアにおいて共存あるいは、隣接可能である。しかし、IPv4ネットワークとIPv6ネットワークとは、異なるネットワーク層アドレス体系を持つため、経路情報に互換性がない

。このため、IPv4ネットワークとIPv6ネットワークとは、異なる経路制御プロトコルにより管理される。

【０００５】

IPネットワークとアップルトークネットワーク：これらはネットワーク層プロトコルとして、各々IP、アップルトーク（米国アップル・コンピュータ社のプロトコル）を用いたネットワークである。これらのアドレス体系、経路情報に互換性は無い。このため、IPネットワークとアップルトークネットワークとは、異なる経路制御ルールにより管理される。

（同一ネットワーク層プロトコルにおけるドメイン）

異なるネットワーク層プロトコルで運用される各ネットワークは、上記の例で示したように、経路情報に互換性がないために、異なるドメインに分割される。

【０００６】

一方、同一ネットワーク層プロトコルで運用される複数のネットワークは、経路情報に互換性があるため、これらのネットワークを一つのドメインにまとめることは原理的には可能である。しかし、実際には、このようなネットワークが、意図的に複数のドメインに分割されることがある。このように同一ネットワーク層プロトコルで運用される複数のネットワークを複数のドメインに分割する理由を以下に例示する。

（例１）独立に運用していた複数のネットワークを接続すると、各ネットワーク内では一意であるように割り振ったネットワーク層アドレスが一意性を失い、経路情報が破綻する場合がある。このような事態を避けるため、各ネットワークが別々のドメインとして定義され、定義されたドメイン同士が接続される。このようにして、各ドメイン内でネットワーク層アドレスを独立に割り振ることが可能になる。

（例２）あるネットワーク1について、外部ネットワークからの侵入に対するセキュリティを強化したい場合、ネットワーク1と外部ネットワークとが、別々のドメインとして分割される。これにより、経路情報などのネットワーク1内の情報を外部ネットワークから隠蔽できるので、外部ネットワークからのネットワーク1への接続が遮断される。

（ネットワークの分割管理に対する要求）

上記のような理由により、組織内と組織外とは異なるドメインとして分割されることが多い。一方、同一組織内では通信の到達性が優先される。そのため、その組織内で共通の経路制御ルールに従いネットワークが運用される場合が多い。

【０００７】

しかし、同一組織内でも、異なる経路制御ルールを用いる範囲を定義することで通信の到達性を制限し、セキュリティや管理上の利便性を優先する場合がある。それは、例えば、同一企業グループ内における企業間ネットワークを構築する場合、同一企業内の特にセキュリティを必要とする部門と他の部門とを接続する場合、同一企業内の関連子会社間を接続する等の場合である。

（従来の技術）

上述のように、従来、ネットワークが同一のネットワーク層プロトコルで運用される場合でも、組織内ネットワークと組織外ネットワークとは異なるドメインとして分割され、同一組織内は、通信の到達性を優先して共通のドメインとされることが多い。従って、同一ネットワーク層プロトコルが用いられているネットワーク上に必要なドメインは、組織内と組織外の高々二つであった。

【０００８】

以下で、組織内のネットワークと組織外ネットワークとを別のドメインとして管理する場合の、組織内と組織外の間に位置する中継装置（以下中継装置１と記す）におけるパケットの中継手順を記す。

【０００９】

まず、中継の前提条件を示す。

［条件１］

組織内網の各ノード（通信装置）は、組織外ノードの名前からそのノードのネットワーク層アドレスを獲得する手段などにより、接続を希望する組織外ノードのネットワーク層アドレスを獲得可能である。

［条件２］

組織内網の各ノードは、組織内で交換する経路情報に、組織内に割り振られたネットワーク層アドレス以外を宛先とするパケットの経路中に中継装置１を含め

る。すなわち、組織内網の各ノードは、組織外のノードへの経路には中継装置１が含まれることを予め知っている。

［条件３］

組織外網の各ノードは、組織内ノードの代理ホストとなる中継装置１への経路情報を予め知っている。この経路情報は、中継装置１の組織外網上のネットワーク層アドレスを宛先とする。

【００１０】

このような場合、中継装置１は、以下のように動作していた。

［動作１］

第１は、中継装置１が、組織内から組織外のネットワーク層アドレスを宛先とするパケットを受信した場合である。この場合、まず、中継装置１は、このパケットの送信元アドレスを組織内ノードの代理ホストとして振舞うために中継装置１に用意したネットワーク層アドレスに変換する。次に、中継装置１は、このパケットを組織外に送信する。これにより、このパケットは、上記代理ホストを送信元として送出される。

［動作２］

第２は、中継装置１が組織外から組織内ノードの代理ホスト用アドレスを宛先とするパケットを受信した場合である。この場合、まず、中継装置１は、該パケットに付与された宛先アドレスを代理ホスト用のネットワーク層アドレスから組織内ノードのネットワーク層アドレスに変換する。次に、中継装置１は、組織内にパケットを中継する。これにより、このパケットは、組織内ノードを宛先として組織内に中継される。

【００１１】

以上で組織内外の二つのドメインを分割する中継装置１の動作を述べた。

しかし、組織内外の定義以外に、組織内にも複数のドメインを定義したい場合がある。このような場合、従来の中継装置は、組織内と組織外という区分以外のドメインを認識できなかった。そのため、多数のドメイン（またはネットワーク）が、上記［条件１］から［条件３］における組織としての条件を満たす場合でも、中継装置は、これらのドメイン対ごとに接続ルールを決定し、その接続ルー

ルに従いドメイン間のパケットの中継を行うような動作はできなかった。

【００１２】

【発明が解決しようとする課題】

本発明はこのような従来の技術の問題点に鑑みてなされたものであり、多数のドメイン（またはネットワーク）が、上記［条件１］から［条件３］における組織としての条件を満たす場合、これらのドメインを定義･管理し、セキュリティや保守の独立性を確保した上で、ドメイン間の制限的な接続機能を提供することを技術的課題とする。

【００１３】

【課題を解決するための手段】

本発明は前記課題を解決するために、以下の手段を採用した。

本発明は、各々１以上の通信装置を接続した、そのような２以上のネットワークを中継する通信データ中継装置であって、

ネットワークにアクセスするための２以上のインターフェース部と、

１以上のネットワークを接続したシステムとしてのドメインを定義するドメイン定義部と、

２以上のドメイン間における接続の可否を定義するドメイン間接続定義部と、

通信データの中継先を記憶する経路情報記憶部と、

異なるドメイン間で通信データを中継するときに、送信側ドメインにおける送信元アドレスと中継先ドメインにおける送信元アドレスとを相互に変換するアドレス変換部と、

ドメイン間接続定義部の定義に従い、２以上のドメイン間における中継の可否を制御する制御部とを備えたものである。

【００１４】

ここで、ドメインとは、１以上のネットワークを接続したシステムであって、本通信データ中継措置が中継する対象をいう。中継の可否を制御するとは、例えば、ドメイン間接続定義テーブルの定義に従って、ドメイン間の接続が許可されている場合には中継し、ドメイン間の接続が許可されていない場合には中継しないことをいう。

【００１５】

送信側ドメインとは、中継装置によって中継される２つのドメインのうち、送信側に位置するドメインをいう。また、中継先ドメインとは、中継装置によって中継される２つのドメインのうち、宛先側に位置するドメインをいう。

【００１６】

このアドレス変換部は、異なるドメイン間で通信データを中継するときに、送信側ドメインにおける送信先アドレスと中継先ドメインにおける送信先アドレスとを相互に変換するものでもよい。

【００１７】

また、ドメイン定義部は、ドメインを、そのドメインに接続されるインターフェース部を識別する情報によって定義してもよい。

また、制御部は、通信データを受信したインターフェース部に対応付けられるドメイン（または通信データを受信したインターフェース部）と、

その通信データの送信元アドレスが属するドメイン（またはその通信データの送信元アドレスが属するドメインに対応付けられるインターフェース部）とが、異なる場合に、その通信データを廃棄してもよい。

【００１８】

また、ドメイン定義部を、各ドメインごとに、そのドメインに含まれるネットワークを識別するアドレス（またはそのドメインに含まれるネットワークに接続される通信装置を識別するアドレス）によって定義してもよい。

【００１９】

【発明の実施の形態】

以下、本発明の好適な実施の形態を図面を参照して説明する。

（第１実施形態）

本発明の第１実施形態を図１から図８の図面に基づいて説明する。

【００２０】

図１は、本実施形態に係るネットワークの構成図であり、図２は、複数のネットワークを接続する中継装置１のハードウェア構成図であり、図３は、この中継装置１の機能構成図であり、図４は、図２に示した中継装置１のＣＰＵ１４で実

行される制御プログラムのフローチャートであり、図５から図８は、この制御プログラムを実行する際にＣＰＵ１４が使用するテーブルのデータ構造を示す図である。

＜ネットワーク構成＞

図１に、第１実施形態に係るネットワークの構成図を示す。このネットワークは、サービスプロバイダの提供する企業外ネットワークＩＳＰ－１（以下ＩＳＰ－１と略す、ＩＳＰ－２も同様）と、中継装置１に中継される企業内ネットワークＬＡＮ－１（以下ＬＡＮ－１と略す、ＬＡＮ－２も同様）及びＬＡＮ－２と、インターネットとを含んでいる。

［ＩＳＰ－１］

ＩＳＰ－１は、サービスプロバイダが提供する企業外ネットワークである。ＩＳＰ－１のネットワークを識別するネットワークアドレスは、140.2.100.0/24である。ＩＳＰ－１には、ルータＡを介してインターネットが接続されている。このルータＡは、ＩＳＰ－１において、アドレス140.2.100.180によって識別される。

［ＩＳＰ－２］

ＩＳＰ－２は、サービスプロバイダが提供する企業外ネットワークである。ＩＳＰ－２のネットワークを識別するネットワークアドレスは、200.2.100.0/24である。ＩＳＰ－２も、ルータＣ２を介してインターネットに接続されている。

［ＬＡＮ－１］

ＬＡＮ－１は、関連会社１の企業内ネットワークである。ＬＡＮ－１のネットワークを識別するネットワークアドレスは、133.160.5.0/24である。ＬＡＮ－１は、ＩＳＰ－１経由でインターネットに接続されている。

［ＬＡＮ－２］

ＬＡＮ－２は、関連会社２の企業内ネットワークである。ＬＡＮ－２のネットワークを識別するネットワークアドレスは、10.25.60.0/24である。ＬＡＮ－２は、ルータＣ１を介してＩＳＰ－２に接続されている。このＩＳＰ－２は、関連会社２が独自に契約したサービスプロバイダが提供するネットワークである。また、

ルータＣ１は、ＬＡＮ－２において、アドレス10.25.60.180によって識別される。さらに、ＬＡＮ－２は、ＩＳＰ－２を経由してインターネットに接続されている。

【００２１】

中継装置１は、ドメイン間を接続するための論理インターフェース（インターフェース部に相当）として、ＩＦ－０、ＩＦ－１、及びＩＦ－２を備えている。上記ネットワークに対して、中継装置１では、以下のようなドメインが定義されている。

［ドメインＡ］

ドメインＡは、ＩＳＰ－１及びインターネットからなる。また、ドメインＡは、論理インターフェースＩＦ－０を介して中継される。ＩＦ－０のネットワークＩＳＰ－１におけるアドレスは、140.2.100.1である。

［ドメインＢ］

ドメインＢは、ＬＡＮ－１からなる。また、ドメインＢは、論理インターフェースＩＦ－１を介して中継される。ＩＦ－１のネットワークＬＡＮ－１におけるアドレスは、133.160.5.1である。

［ドメインＣ］

ドメインＣは、ＬＡＮ－２からなる。ただし、上述のようにＬＡＮ－２はインターネットに接続されている。また、ドメインＣは、論理インターフェースＩＦ－２を介して中継される。ＩＦ－２のネットワークＬＡＮ－２におけるアドレスは、10.25.60.1である。

【００２２】

本第１実施形態では、中継装置１経由の通信の接続ポリシを以下のように想定する。

（１）関連会社１（ＬＡＮ－１）からＩＳＰ－１への接続、及びＩＳＰ－１経由でのインターネットへの接続は許可される。

（２）関連会社１（ＬＡＮ－１）から関連会社２（ＬＡＮ－２）への接続は許可される。

（３）他のドメイン間接続は全て非許可とする。

以下、このような接続を実現する中継装置１の構成と、その処理とについて説明する。

＜中継装置１のハードウェア構成＞

図２に本実施形態に係る中継装置１のハードウェア構成図を示す。

【００２３】

この中継装置１は、制御プログラムやデータを記憶するメモリ１３と、メモリ１３に記憶された制御プログラムを実行するＣＰＵ１４（制御部に相当）と、ＣＰＵ１４から制御されて他の通信装置と通信する複数の物理インターフェース１５ａ、１５ｂ、１５ｃ等とを備えている。

【００２４】

メモリ１３は、ＣＰＵ１４が実行する制御プログラムやＣＰＵ１４が処理するデータを記憶する。

ＣＰＵ１４は、メモリ１３に記憶された制御プログラムを実行し、中継装置１としての機能を提供する。

【００２５】

物理インターフェース１５ａ、１５ｂ、１５ｃは、ＣＰＵ１４からの指令により通信データをネットワーク１０に送出し、またはネットワークから通信データを受信する。

＜機能構成＞

図３に中継装置１の機能構成を示す。中継装置１の機能は、メモリ１３に記憶されるドメイン定義テーブル２（ドメイン定義部に相当）、ドメイン間接続定義テーブル４（ドメイン間接続定義部に相当）、アドレス変換テーブル７、及び経路情報テーブル１０（経路情報記憶部に相当）と、ＣＰＵ１４の制御プログラムとして実行されるドメイン定義手段２ａ、ドメイン間接続判定手段４ａ、アドレス変換手段７ａ及びアドレス逆変換手段７ｂによって提供される。

［ドメイン定義テーブル２］

ドメイン定義テーブル２は、ドメインと１以上の論理インタフェースＩＦ－０等とを対応付けるテーブルである。論理インターフェースとは、中継装置１の制御プログラムが各ドメインと通信する際のインターフェースの識別情報である。

本第１実施形態では、論理インターフェースは、図２に示した物理インターフェース１５ａ、１５ｂまたは１５ｃのいずれかを通じてドメインに接続される論理的な端子を示している。

【００２６】

図５に図１のネットワーク構成に対するドメイン定義テーブル２の設定内容を示す。図５のように、ドメインＡ、Ｂ及びＣは、各々通信の論理インターフェース番号ＩＦ－０、ＩＦ－１及びＩＦ－２によって定義される。すなわち、中継装置１は、論理インターフェースＩＦ－０、ＩＦ－１及びＩＦ－２を介する通信データを、各々ドメインＡ、Ｂ及びＣに含まれるノードとの通信データとして中継する。

［ドメイン間接続定義テーブル４］

ドメイン間接続定義テーブル４には、複数のドメインのうち、任意の一組のドメイン毎の通信可否、及び通信が許可されているドメイン間の接続時に用いられるアドレス変換手法が定義される。ドメイン間接続定義テーブル４は、ドメイン定義手段２ａを用いて設定される。

【００２７】

図６に、図１のネットワークにおけるドメイン間接続定義テーブル４の定義を示す。

図６で、「Ｎ」はNAT（IP Network Address Translator）を施して接続を許可することを示す。NATとはアドレス変換機能の一種であり、NATにより送信元IPアドレスが中継装置１上のIPアドレスで置換されてパケットが中継される。その結果、この中継装置１が送信先ネットワーク上で代理ホストとして振舞う。

【００２８】

図６で、「×」は接続非許可を示す。

また、「－」はパケットのフォワード処理による通常の接続（同一ドメイン内接続）を示す。

［アドレス変換テーブル７］

アドレス変換テーブル７は、送信元ドメインにおけるアドレス変換前の送信元のＩＰアドレスと、宛先ドメインにおけるアドレス変換後のＩＰアドレスとを対

応付けるテーブルである。図７に、本実施形態におけるアドレス変換テーブル７の登録内容の例を示す。

［経路情報テーブル１０］

経路情報テーブル１０には、パケットを中継する際に、そのパケットを次に転送（これをホップという）すべきノードのアドレスが定義される。

【００２９】

図８に、本実施形態における経路情報テーブル１０の構成を示す。図８のように、この経路情報テーブル１０は、宛先ＩＰアドレス、ネットマスク、次ホップノードのＩＰアドレス（中継先に相当）、及び送信論理インターフェースが含まれている。

【００３０】

図８において、「次ホップノードのIPアドレス」における「－」は、宛先ネットワークが物理インタフェース１５ａ等から直接到達可能であることを示す。

また、図８において、「宛先IPアドレス」を「0.0.0.0」とするエントリは、デフォルトルートを示している。このデフォルトルートとは、経路情報テーブル１０を検索した結果、宛先ＩＰアドレスが他のいずれのエントリにも合致しないパケットに対する中継先を示す。

【００３１】

なお、ISP-1に接続されたインターネットとISP-2に接続されたインターネットの両方を中継装置１が意識すると経路情報が混乱する。そこで、中継装置１はドメインＣの経路情報として、LAN-2の経路情報のみを認識するように設定される。

【００３２】

また、中継装置１は、中継装置１に接続された全ドメイン（ドメインＡ，Ｂ，Ｃ）の情報を、経路情報テーブル１０のように予め知っているものとする。

また、ドメイン間接続定義テーブル４では、ドメインＢからドメインＡへの通信及びドメインＢからドメインＣへの通信を許可している。この場合、ドメインＢは、中継装置１から経路情報テーブル１０を経路情報として得ることにより、予めドメインＡ、Ｃの経路情報を知っているものとする。

［ドメイン定義手段２ａ］

ドメイン定義手段２ａは、論理インタフェースＩＦ－０、ＩＦ－１、ＩＦ－２等とドメインとを対応付けるドメイン定義テーブル２、及びドメイン間の接続を定義するドメイン間接続定義テーブル４を定義する際に使用される。このドメイン定義手段２ａは、制御プログラムの一機能であり、ユーザがネットワークを介して中継装置１のＣＰＵ１４にログインすると実行される。ドメイン定義手段２ａは、起動されると、ネットワークを介してユーザの端末画面に不図示のドメイン定義テーブル設定画面及び不図示のドメイン間接続定義テーブル設定画面を表示し、ユーザに設定を促す。

［ドメイン間接続判定手段４ａ］

ドメイン間接続判定手段４ａは、複数のドメインのうち、任意の一組のドメイン毎の通信可否を判定し、接続時に用いるアドレス変換手法を決定する。ドメイン間接続判定手段４ａは、ＣＰＵ１４で実行される制御プログラムの機能として実現される。

［アドレス変換手段７ａ］

アドレス変換手段７ａは、アドレス変換テーブル７に基づいて、パケットを中継するときに、パケットヘッダ内の送信元アドレスを変換する。

【００３３】

変換前の送信元アドレスがアドレス変換テーブル７に定義されていない場合には、アドレス変換手段７ａは、その送信元アドレスに対する定義をアドレス変換テーブル７に追加する。

【００３４】

すなわち、アドレス変換手段７ａは、送信元ドメインから到着したパケットの送信元アドレスに対し、宛先側ドメインで使用可能な、本装置でプールしてある宛先ドメイン内のアドレスを対応付ける。また、アドレス変換手段７ａは、このアドレスの対応付けをアドレス変換テーブル７に書き込む。

［アドレス逆変換手段７ｂ］

アドレス逆変換手段７ｂは、宛先ドメインから送信元ドメインへ向かう返信パケットをアドレス変換テーブル７の情報に基づき変換する。

【００３５】

アドレス変換手段７ａは、ＣＰＵ１４で実行される制御プログラムの機能として実現される。

［パケット受信手段８］

パケット受信手段８は、論理インターフェースＩＦ－０、ＩＦ－１、ＩＦ－２等を監視し、パケットを受信する。パケット受信手段８は、ＣＰＵ１４で実行される制御プログラムの機能として実現される。

［パケット送信手段９］

パケット送信手段９は、経路制御情報テーブル１０を参照し、論理インターフェースＩＦ－０、ＩＦ－１、またはＩＦ－２を通じてパケットの送信を指令する。パケット送信手段９は、ＣＰＵ１４で実行される制御プログラムの機能として実現される。

【００３６】

以上の手段を用いた動作について、以下に示す。

中継装置１がネットワーク層パケットを受信すると、中継装置１は、アドレス変換手段７ａによって、アドレス変換テーブル７を検索する。アドレス変換テーブル７に、その送信元アドレスが存在した場合は、中継装置１は、アドレス変換テーブル７に登録された変換前アドレス／変換後アドレスに従い、送信元アドレスを変換する。

【００３７】

アドレス変換テーブル７に、その送信元アドレスが存在しない場合には、中継装置１は、逆アドレス変換手段７ｂを使用する。すなわち、中継装置１は、アドレス変換テーブル７の変換前情報と、変換後情報とを置き替えて検索する。置き換えて検索した結果、情報が存在した場合には、中継装置１は、このパケットを応答パケットであると判断する。そして、中継装置１は、アドレス変換テーブル７の変換前アドレス／変換後アドレスに従いアドレス逆変換を行う。

【００３８】

変換前情報と、変換後情報を置き替えて検索しても、アドレスがアドレス変換テーブル７で検出できない場合には、中継装置１は、このパケットの送信元から

受信先へのドメインをまたがる通信はまだ行われたことが無いと判断する。そこで、中継装置１は、本パケットがドメインをまたがる通信かどうかを調べる。先ず、中継装置１は、送信元アドレス／宛先アドレスや受信論理インタフェースＩＦ－０等から、ドメイン定義テーブル２を参照し、送信元ドメインと宛先ドメインとを決定する。

【００３９】

送信元ドメインと宛先ドメインが異なる場合は、中継装置１は、ドメイン間接続判定手段４ａにより、ドメイン間接続定義テーブル４を参照し、宛先ドメインへ中継するかどうか、及びどのアドレス変換手法を用いるかを決定する。この結果に基づき、中継装置１は、変換前の送信元アドレス、変換後の送信元アドレスの対応関係をアドレス変換テーブル７へ登録する。

【００４０】

以上の動作により、中継装置１に接続された異なる様々なドメイン間の中継が可能となる。

＜作用・効果＞

図４のフローチャートに、この中継装置１の動作を示す。中継装置１のＣＰＵ１４は、メモリ１３に記憶した制御プログラムを実行し、中継装置１の機能を提供する。

【００４１】

まず、ドメインＢ上のホストｂ（IPアドレス133.160.5.2）から、ドメインＣ上にあるホストｃ（IPアドレス10.25.60.99）にパケットを中継する際の処理について説明する。ドメインＢからドメインＣへの接続については、ドメイン間接続定義テーブル４によりNAT処理を施して接続することが許可されているため（図６）、本パケットの処理は以下のようになる。

【００４２】

1.｛送信元IPアドレス、宛先IPアドレス｝の対を｛133.160.5.2、10.25.60.99｝とするパケットについて、中継装置１は、パケットの宛先IPアドレスが中継装置１の論理インタフェースと対応する場合、本パケットが中継装置１宛であると判断し、該論理インタフェースでパケットを受信する。しかし、本動作例ではパ

ケットの宛先IPアドレスが中継装置１の論理インタフェースと対応しない。そのため、中継装置１は、フレームを受信した物理インタフェース上の、フォワード可能な論理インタフェースＩＦ－１からパケットを受信する（ステップＳ１、以下Ｓ１と略す）。

【００４３】

2.次に中継装置１は、 アドレス変換テーブル７中で、パケットの宛先IPアドレス「10.25.60.99」が変換前IPアドレスと一致するエントリを検索する。この検索がヒットした場合（Ｓ２の判定でヒットの場合）、中継装置１はパケットの送信元IPアドレスをアドレス変換テーブル７中の変換後IPアドレス「10.25.60.2」で置換する（Ｓ３）。

【００４４】

3．中継装置１は、経路情報テーブル１０から宛先IPアドレス「10.25.60.99」をキーとして検索する（経路選択処理）。その結果、中継装置１は、送信論理インタフェースとしてＩＦ－２を獲得するとともに、本パケットを次に送る宛先ノードはＩＦ－２から直接到達可能であることを知る（Ｓ４）。以上の結果、中継装置１は、このＩＦ－２を介して、宛先ノードに対しパケットを送信する（Ｓ５）。

【００４５】

4．アドレス変換テーブル７の検索がヒットしなかった場合（Ｓ２の判定でミスヒットの場合）、中継装置１は、アドレス変換テーブル７の変換前情報と、変換後情報とを置き替えて検索する（Ｓ６）。

【００４６】

5．このパケットは返信パケットではないので、アドレス変換テーブル７の変換前情報と、変換後情報とを置き替えても検索はヒットしない（Ｓ６の判定でミスヒットの場合）。そこで、このパケットに指定のドメインをまたがる通信はまだ行われていないことが分かる。その場合、中継装置１は、このパケットにドメインをまたがる宛先が指定されているか否かを以下のように調べる。

【００４７】

まず、中継装置１は、装置内の経路情報テーブル１０を宛先IPアドレス「10.2

5.60.99」をキーとして検索する（経路選択処理）。その結果、中継装置１は、送信論理インタフェースとしてＩＦ－２を獲得するとともに、本パケットを次に送る宛先ノードはＩＦ－２から直接到達可能であることを知る（Ｓ７）。

【００４８】

6．次に、中継装置１は、ドメイン定義テーブル２を参照することにより、受信論理インタフェースＩＦ－１と送信論理インタフェースＩＦ－２に対応するドメインとして、受信ドメインＢと送信ドメインＣを獲得する（Ｓ８）。

【００４９】

7.次に中継装置１は、受信ドメインと送信ドメインとが同一か否かを判定する（Ｓ９）。受信ドメインと送信ドメインとが異なる場合には（Ｓ９の判定でNOの場合）、中継装置１は、このパケットがドメインをまたがるものであると判断する。

【００５０】

そこで、中継装置１は、ドメイン間接続定義テーブル４を参照して（Ｓ１０）、ドメインＢからドメインＣへの接続の可否を判定する（Ｓ１１）。本実施例では、ドメインＢからドメインＣへの接続ポリシはNATによる接続であるため（Ｓ１１）、中継装置１は、本パケットに対してNAT処理を施す（Ｓ１２）。次に、中継装置１は、アドレス変換テーブル７に変換前アドレスと変換後アドレスの対応を登録し（Ｓ１３）、その後、本論理インタフェースＩＦ－２から送信する（Ｓ５）。

【００５１】

以上の手順により、中継装置１はドメインＢからドメインＣへのパケットの中継を行う。なお、Ｓ９の判定で、受信ドメインと送信ドメインとが一致する場合には（Ｓ９の判定でYESの場合）、中継装置１は、送信論理インターフェースからそのままパケットを送出する（Ｓ５）。

【００５２】

次に、このパケットに対する応答パケットがホストｃから帰ってきたときの動作を示す。

8．｛送信元IPアドレス、宛先IPアドレス｝の対を｛10.25.60.99、10.25.60.2

｝とするパケットについて、パケットの宛先IPアドレスが中継装置１の論理インタフェースと対応する場合には、中継装置１は、本パケットが中継装置１宛であると判断し、該論理インタフェースでパケットを受信する。しかし、受信したパケットの宛先IPアドレスが中継装置１の論理インタフェースと対応しないため、中継装置１は、フレームを受信した物理インタフェース上の、フォワード可能な論理インタフェースＩＦ－２からパケットを受信する（Ｓ１）。

【００５３】

9．次に中継装置１は、アドレス変換手段７ａにより、アドレス変換テーブル７中で、パケットの宛先IPアドレス「10.25.60.2」が変換前IPアドレスと一致するエントリを検索する（Ｓ２）。

【００５４】

この場合、検索はヒットしないため、中継装置１は、更にアドレス逆変換手段７ｂにより、アドレス変換テーブル７中の変換前IPアドレスと変換後IPアドレスを置き換えて検索する（Ｓ６）。この2回目の検索はヒットするので、中継装置１は、検索結果に従い、パケットの宛先IPアドレス「10.25.60.2」をアドレス変換テーブル７中の変換前IPアドレス「133.160.5.2」で置換する（Ｓ１５）。

【００５５】

10．次に中継装置１は、装置内の経路情報テーブル１０から宛先IPアドレス「133.160.5.2」をキーとして検索する（経路選択処理）。その結果送信先の論理インタフェースとしてＩＦ－１を獲得するとともに、本パケットを次に送る宛先ノードはＩＦ－１から直接到達可能であることを知る（Ｓ４）。さらに、中継装置１は、このＩＦ－１を介して、パケットの送信処理を行う（Ｓ５）。

【００５６】

以上の処理により、ドメインＣからドメインＢへのパケットの中継を行う。

以上の（1）～（10）の動作をすることにより、中継装置１は、ドメインＢからドメインＣへの通信を可能とする。

【００５７】

なお、ドメインＢがドメインＡ、Ｃの経路情報を知っているものとすることは先に述べたが、これは以下のａ）またはｂ）のいずれかにより実現される。

ａ）中継装置１が、以下の11.(A)～(C)の基準に基づき、経路情報を各ドメインと交換している。

ｂ）各ドメイン内で、経路情報を以下の11.(A)～(C)の基準に基づき設定している。

11．ドメイン間の接続定義がドメイン間接続定義テーブル４のような設定の場合、ドメイン定義テーブル２にて定義されている各ドメインＡ、Ｂ、Ｃに必要な経路情報の決定基準を以下に示す。

【００５８】

Ａ）ドメインＡの経路情報の決定基準：

ドメインＡからの接続を許可するドメインは、ドメインＡのみであるため、経路情報テーブル１０に登録された経路情報のうちでドメインＡに通知される経路情報は、送信論理インタフェースがＩＦ－０である経路情報のみである。なお、中継装置１はドメインＡとは経路情報の交換が可能である。

【００５９】

Ｂ）ドメインＢの経路情報の決定基準：

ドメインＢからの接続を許可するドメインは、ドメインＡ，Ｃ、及びドメインＢ自身であるため、経路情報テーブル１０に登録された経路情報のうちでドメインＢに通知される経路情報は、基本的に経路情報テーブル１０のすべてである。但し、インターネット上の全経路情報を企業内ネットワーク内に流すと、情報量が多くなって、経路情報テーブル１０が破綻する。そこで、企業内ネットワークには企業外の情報としては、デフォルトルート（宛先IPアドレス＝0.0.0.0のエントリ）の情報のみが通常流される。なお、中継装置１はドメインＢとは経路情報の交換が可能である。

【００６０】

Ｃ）ドメインＣの経路情報の決定基準：

ドメインＣは独自にインターネットと接続しており、ドメインＡ上のインターネットとドメインＣに接続されたインターネットの両方を中継装置１が意識すると経路情報が混乱する。そのため、中継装置１はドメインＣとは経路情報を交換せずに、ドメインＣへの経路情報を静的に設定する。

【００６１】

以上により、ドメイン間接続定義テーブル４で設定したようなドメイン間の接続が可能となる。

＜論理インターフェースの変形＞

上記第１実施形態では、中継装置１は、論理インターフェースＩＦ－０、ＩＦ－１、またはＩＦ－２を介して各ドメインと対応付けられた。しかし、本発明の実施は、このような構成には、限定されない。例えば、論理インターフェースＩＦ－０等を介さず、直接物理インターフェース１５ａ、１５ｂ、または１５ｃを各ドメインに対応付けてもよい。この場合は、物理インターフェースがインターフェース部に相当する。

【００６２】

このように、物理インターフェース１５ａ、１５ｂ、または１５ｃを各ドメインに対応付けた場合、フレームを受信した物理インタフェースでパケットを受信し、送信元のドメインを決定する。

＜アドレス変換の変形＞

上記第１実施形態では図７のように、アドレス変換テーブル７に変換前ＩＰアドレスと変換後ＩＰアドレスとを登録した。しかし、本発明の実施は、アドレス変換テーブル７の構成には限定されない。例えば、アドレス変換テーブル７の構成として、パケットヘッダの情報、送受信論理インターフェースに係る情報、送受信物理インターフェースに係る情報、あるいは、送受信ドメインに係る情報等を含めてもよい。

【００６３】

また、上記実施形態では、アドレス変換手段７ａは、送信元ドメインから到着したパケットの送信元アドレスに対し、宛先側ドメインで使用可能な、本装置でプールしてある宛先ドメイン内のアドレスを対応付ける。これに代えて、アドレス変換手段７ａが、送信元ドメインから到着したパケットのヘッダ情報に対し、宛先側ドメインで使用可能な、本装置でプールしてあるネットワーク層／トランスポート層のヘッダ情報を対応付けるようにしてもよい。例えば、以下のようなアドレス変換手段NAPTなどを用いてもよい。

Ａ）アドレス変換時には、パケットの「送信元IPアドレス、送信元ポート番号、宛先IPアドレス、宛先ポート番号、ＩＰヘッダ中の上位プロトコル番号、変換後送信元IPアドレス、変換後宛先ポート番号」の組をアドレス変換テーブル７に記憶し、「送信元IPアドレス、送信元ポート番号、宛先IPアドレス、宛先ポート番号、ＩＰヘッダ中の上位プロトコル番号」の組がパケットのそれと一致するエントリを検索して、パケットの「送信元IPアドレス、送信元ポート番号」をアドレス変換テーブル７中の「変換後送信元IPアドレス、変換後送信元ポート番号」で置換して論理インタフェースからパケットを送信する。

Ｂ）アドレス逆変換時には、パケットの「宛先IPアドレス、宛先ポート番号、送信元IPアドレス、送信元ポート番号、ＩＰヘッダ中の上位プロトコル番号」がアドレス変換テーブル７中の「変換後送信元IPアドレス、変換後送信元ポート番号、宛先IPアドレス、宛先ポート番号、ＩＰヘッダ中の上位プロトコル番号」の組と一致するエントリを探して、ヒットした場合にパケットの「宛先IPアドレス、宛先ポート番号」をアドレス変換テーブル７中の「送信元IPアドレス、送信元ポート番号」で置換して論理インタフェースからパケットを送信する。

＜その他の変形例＞

上記第１実施形態では、ネットワーク層のアドレスとして、ＩＰアドレスを用いるネットワークにおいて本発明を実施する例を説明した。しかし、本発明の実施は、ＩＰによるネットワークに限定されるものではない。例えば、ＩＰＸを用いたネットワークの中継においても本発明を実施をできる。

【００６４】

上記第１実施形態では、ドメインと各論理インターフェースＩＦ－０等を対応付けるドメイン定義テーブル２を使用した。しかし、本発明の実施は、ドメインを定義する情報の構造には限定されない。例えば、テーブルではなく、論理インタフェースごとにドメインを識別する情報を１以上列記する構造体に、ドメインを定義する情報を保持してもよい。

【００６５】

上記第１実施形態では、ドメイン間接続判定手段４ａ、アドレス変換手段７ａ及びアドレス逆変換手段７ｂをＣＰＵ１４の制御プログラムとして構成した。し

かし、本発明の実施は、このような構成には限定されない。例えば、これらの処理を実行する専用ＬＳＩを用いてもよい。

【００６６】

上記実施形態では、ドメイン定義テーブル２及びドメイン間接続定義テーブル４の内容を定義するため、ドメイン定義手段２ａを用いた。しかし、本発明の実施において、ドメイン定義手段２ａは必須の構成要素ではない。例えば、中継装置１が、特定のノード（サーバ）のハードディスク上からドメイン定義テーブル２及びドメイン間接続定義テーブル４の内容を読み取るようにすれば、ドメイン定義手段２ａは使用しなくてもよい。

（第２実施形態）

上記第１実施形態では、ドメイン定義テーブル２を各ドメインと、そのドメインに接続される論理インターフェースＩＦ－０等とによって定義した。本第２実施形態では、ドメイン定義テーブル２を各ドメインと、そのドメインに含まれるネットワークのアドレスとによって定義する例を示す。

【００６７】

図９は、この場合のドメイン定義テーブル２の定義例であり、図１０は、認証サーバと中継装置１との組み合わせによるネットワークの構成図である。これら以外の構成については、第２実施形態は、第１実施形態と同様である。そのため、他の構成については、図１から図４あるいは図６から図８の図面を参照して説明する。

＜構成＞

図９にドメイン定義テーブル２の定義例を示す。図９のように本第２実施形態では、ドメイン定義テーブル２は、ＩＰアドレス、ネットマスク、及びドメインを識別する情報を有している。例えば、ドメインＡは、ＩＰアドレスが140.2.100.0でネットマスクが255.255.255.0であるネットワークを有している。ドメインが複数のネットワークを含む場合には、この関係（そのネットワークのＩＰアドレス、ネットマスク、及びドメインＡを識別する情報）がドメイン定義テーブル２に列記される。

【００６８】

また、図９の最下段において、ＩＰアドレスが0.0.0.0であるエントリが定義されている。これは、この定義部分より上段のエントリで定義されたＩＰアドレスのいずれにも該当しないパケットのアドレスは、すべてドメインＡに属することを意味する。

＜作用・効果＞

上記のように本第２実施形態は、ドメイン定義テーブル２の構成以外は、第１実施形態と同様であるので、中継装置１の処理は、図４によって示される。以下、中継装置１の処理を説明する。

【００６９】

1．第２実施形態においても、中継装置１は、第１実施形態の1.から5.までと同様の処理を実行する。

2．ただし、第２実施形態では、第１実施形態の6.のように論理インタフェースによりドメインを認識する代わりに、中継装置１は、パケットの送信元IPアドレスと宛先IPアドレスとから、送信元ドメインＢと宛先ドメインＣを得る（Ｓ８）。

【００７０】

3．さらに、中継装置１は、第１実施形態の7.から10.までと同様の処理を実行する。

なお、第１実施形態と同様、ドメインＢはドメインＡ、Ｃの経路情報を知っているものとする。これは以下のｃ）またはｄ）のいずれかにより実現される。

ｃ）中継装置１が、以下の12.(A)～(C)の基準に基づき、経路情報を各ドメインと交換している。

ｄ）各ドメイン内で、経路情報を以下の12.(A)～(C)の基準に基づき設定している。

【００７１】

12．ドメイン間の接続定義がドメイン間接続定義テーブル４のような設定の場合、ドメイン定義テーブル２にて定義されている各ドメインＡ、Ｂ、Ｃに必要な経路情報の決定基準は以下の通りである。

【００７２】

Ａ）ドメインＡの経路情報の決定基準：

ドメインＡからの接続を許可するドメインは、ドメインＡのみであるため、経路情報テーブル１０に登録された経路情報のうちでドメインＡに通知される経路情報は、宛先IPアドレスがドメインＡに含まれる経路情報のみである。なお、中継装置１はドメインＡとは経路情報の交換が可能である。

【００７３】

Ｂ）ドメインＢの経路情報の決定基準：

ドメインＢからの接続を許可するドメインは、ドメインＡ、Ｃ、及びドメインＢ自身であるため、経路情報テーブル１０に登録された経路情報のうちでドメインＢに通知される経路情報は、基本的には経路情報テーブル１０の全てである。但し、インターネット上の全経路情報を企業内ネットワーク内に流すと、情報量が多くなり、経路情報テーブル１０が破綻する。そこで、企業内ネットワークには企業外の情報としては、デフォルトルート（宛先IPアドレス＝0.0.0.0のエントリ）の情報のみが通常流される。なお、中継装置１はドメインＢとは経路情報の交換が可能である。

【００７４】

Ｃ）ドメインＣの経路情報：

ドメインＣは独自にインターネットと接続しており、ドメインＡ上のインターネットとドメインＣに接続されたインターネットの両方を中継装置１が意識すると経路情報が混乱する。そこで、中継装置１はドメインＣとは経路情報を交換せずにドメインＣへの経路情報を静的に設定する。

【００７５】

以上により、第１実施形態と同様に、制限的なドメイン間の接続が可能となる。

＜認証サーバとドメイン接続機能の組み合わせ＞

上記で説明した制限的にドメイン間を接続する中継装置１を認証サーバと組み合わせて使用することにより、さらにセキュリティを確保したドメイン間の制限的な接続が可能になる。

【００７６】

図１０に、このようなネットワークの構成図を示す。

ドメインを異にする関連会社1のネットワーク３１と関連会社２のネットワーク３２とは、上記第２実施形態（または上記第１実施形態）に示した中継装置１によって接続されている。ただし、ネットワーク３１とネットワーク３２とは、異なるドメインに分割され、通常、各関連会社１、２は、互いに他の関連会社への経路情報を持たない。

【００７７】

ここで、関連会社1から関連会社2に出向中のユーザ３０ｂが、セキュリティを確保した上で、関連会社１のネットワーク３１内のノードにアクセスするためのネットワークの接続方法を説明する。

【００７８】

本来、このユーザはネットワーク３１上のユーザ３０ａとしてネットワーク３１内のノード３３に経路３５によりアクセスしていた。しかし、現在は、このユーザは関連会社２のネットワーク３２上のユーザ３０ｂとして接続されている。

【００７９】

この場合、ユーザ３０ｂは、関連会社２上の認証サーバ３４に認証３６を依頼する。ユーザ３０ｂが認証３６に成功した場合、サーバ３４は、中継装置１がネットワーク３１上のノード３３の代理として振る舞うネットワーク層アドレスＡを動的に作成するように中継装置１に依頼する。サーバ３４は、その作成されたネットワーク層アドレスＡをユーザ３０ｂに通知する。このネットワーク層アドレスＡは、中継装置１によってネットワーク３１上のノード３３のアドレスに変換される。

【００８０】

従って、ユーザ３０ｂは、この中継装置１上に動的に作成されたネットワーク層アドレスＡに接続することにより、経路３７により関連会社1上のネットワーク３１との通信可能となる。

【００８１】

一方、上記認証が成功しない場合には、中継装置１上のアドレスが通知されないので、ネットワーク３１のセキュリティが確保される。

このように、本第２実施形態の中継装置１と認証サーバ３４とを組み合わせることにより、多数のネットワーク間で、セキュリティを確保した接続が実現される。なお、この認証サーバ３４と第１実施形態の中継装置１とを組み合わせても、作用及び効果は本第２実施形態の場合と同様である。

＜その他の変形例＞

上記第２実施形態では、ＩＰアドレスとネットマスクとによって、ドメインに含まれるネットワークを指定することで、ドメイン定義テーブル２を定義した。しかし、本発明の実施は、このようなドメイン定義テーブル２のネットワークの指定の仕方には限定されない。例えば、ＩＰアドレスの上限値と下限値により各ドメインに含まれるネットワークを指定してもよい。各ドメインに含まれるすべてのノードのＩＰアドレスを列記することでドメインを定義してもよい。

【００８２】

上記第２実施形態では、ネットワーク層プロトコルとして、ＩＰを使用するネットワークに本発明を適用する例を示した。しかし、本発明の実施は、中継装置においてアドレス変換が可能なネットワーク層であればネットワーク層プロトコルの種類には限定されない。

【００８３】

上記第２実施形態では、ドメイン間接続判定手段４ａ、アドレス変換手段７ａ及びアドレス逆変換手段７ｂをＣＰＵ１４の制御プログラムとして構成した。しかし、本発明の実施は、このような構成には限定されない。例えば、これらの処理を実行する専用ＬＳＩを用いてもよい。

（第３実施形態）

上記第１実施形態においては、ドメイン定義テーブル２を各ドメインと、そのドメインに接続される論理インターフェースＩＦ－０、ＩＦ－１、ＩＦ－２等とによって定義することで、ドメイン間の制限的な接続を可能にする例を示した。本第３実施形態においては、このようなドメイン定義テーブル２を用いたドメイン間のパケットの中継において、不正なパケットを検出し、これを廃棄する処理の例を示す。

【００８４】

図１１は、本第３実施形態に係るネットワーク構成図であり、図１２は、第３実施形態におけるドメイン間接続定義テーブル４の設定例であり、図１３は、この場合の中継装置１の機能構成図であり、図１４は、第３実施形態における中継装置１の処理を示すフローチャートである。第３実施形態の他の構成は、第１実施形態と同様であるので、同一の構成については同一の符号を付して、その説明を省略する。

＜構成＞

図１１に示すように、第１実施形態の場合と異なり、ドメインＣは独自にインターネットへの接続経路を持たず、ドメインＢと同様にＩＳＰ－１経由でインターネット接続されている。

【００８５】

図１２に、この接続ポリシに対するドメイン間接続定義テーブル４の設定を示す。図１２のように、ドメインＡは、ドメインＡ自身に対してのみ送信可能であり、ドメインＢは、ドメインＢ自身の他、ドメインＡ及びＣに対して送信可能であり、ドメインＣは、ドメインＣ自身の他、ドメインＡに対して送信可能である。

【００８６】

ここで、仮にドメインＢからドメインＡに対し、送信元をドメインＣとするパケットが流れた場合、このパケットは不正パケットであるにも関わらず、誤ってアドレス変換されてドメインＡに送信されてしまう恐れがある。これを防ぐために、第１実施形態で説明した処理に加えて、中継装置１が、パケットを受信した論理インタフェースに対応付けられるドメインと、パケットの送信元IPアドレスが属するドメインが異なるかどうかを判別する処理を実行する。そして、この２つのドメインが異なる場合には、中継装置１が、そのパケットを廃棄するパケットフィルタ手段１２を制御プログラムに備えている。

【００８７】

図１３に、本第３実施形態における機能構成図を示す。図１３の構成は、パケットフィルタ手段１２が追加されている点を除いて、第１実施形態の機能構成（図３）と同様である。すなわち、本実施形態では、パケット受信手段８が受信し

たパケットを中継する前に、パケットフィルタ手段１２が、不正パケットを廃棄する。

＜作用・効果＞

図１４に、中継装置１のパケットフィルタ手段１２の処理を示す。ここでは、上述のようにドメインＢに属するノードからドメインＡに属するノードに宛てたパケットが不正であった場合を想定する。このパケットには、ドメインＣに属するノードのアドレスが送信元アドレスとして誤って設定されおり、ドメインＢから論理インターフェースＩＦ－１を介して中継装置１に転送されたものと仮定する。

【００８８】

1．中継装置１は、受信パケットの送信元IPアドレスを経路情報テーブル１０から検索して、そのIPアドレスに対応する論理インタフェースＩＦ－０等を獲得する（Ｓ２０）。

【００８９】

この場合、送信元ノードは、ドメインＣに属するので、中継装置１は、経路情報テーブル１０から論理インタフェースＩＦ－２を獲得する。

2.一方、中継装置１は、第１実施形態で示したドメイン定義テーブル２（図５）を参照して、上記論理インタフェースＩＦ－２に対応するドメインＣを獲得する（Ｓ２１）。

【００９０】

3．次に、中継装置１は、このパケットを実際に受信した論理インタフェースＩＦ－１が属するドメインＢをドメイン定義テーブル２から求める（Ｓ２２）。

4.次に、中継装置１は、Ｓ２１で求めた結果とＳ２２で求めた結果とが一致するか否かを判定する（Ｓ２３）。この結果が一致する場合には、このパケットは、アドレス変換手段へ渡される。

【００９１】

一方、この結果が一致しない場合には、本パケットはパケットの送信元ドメインが、送信元であるべきドメインとは異なるドメインから送信された不正なパケットであるので、中継装置１は、これを廃棄する（Ｓ２５）。

【００９２】

以上により、送信元IPアドレスとして不正な値を持つパケットを、誤って中継することを回避することができる。

＜変形例＞

上記第３実施形態では、ドメイン間接続判定手段４ａ、アドレス変換手段７ａ、アドレス逆変換手段７ｂ、及びパケットフィルタ手段１２をＣＰＵ１４の制御プログラムとして構成した。しかし、本発明の実施は、このような構成には限定されない。例えば、これらの処理を実行する専用ＬＳＩを用いてもよい。

【００９３】

【発明の効果】

以上説明したように、本発明によれば、ネットワーク間を中継する通信データ中継装置において、１以上のネットワークを接続したシステムとしてのドメインを定義するドメイン定義部と、複数のドメイン間における接続の可否を定義するドメイン間接続定義部とを備え、ドメイン間接続定義部の定義に従い複数のドメイン間における中継の可否を制御するので、セキュリティや保守の独立性を確保した上でドメイン間を接続することができる。

【図面の簡単な説明】

【図１】本発明の第１実施形態におけるネットワーク構成図。

【図２】中継装置１のハードウェア構成図。

【図３】中継装置１の機能構成図。

【図４】中継装置１の処理を示すフローチャート。

【図５】ドメイン定義テーブル２の構造を例示する図。

【図６】ドメイン間接続定義テーブル４の構造を例示する図。

【図７】アドレス変換テーブルの構造７を例示する図。

【図８】経路情報テーブル１０の構造を例示する図。

【図９】ドメイン定義テーブル２の構造を例示する図。

【図１０】認証サーバと中継装置１との組み合わせによるネットワークの構成図。

【図１１】第３実施形態のネットワーク構成図。

【図１２】ドメイン間接続定義テーブル４の構造を例示する図。

【図１３】第３実施形態の中継装置１の機能構成図。

【図１４】パケットフィルタ手段１２の処理を示すフローチャート。

【符号の説明】

２　　ドメイン定義テーブル

４　　ドメイン間接続定義テーブル

７　　アドレス変換テーブル

１０　　経路制御テーブル

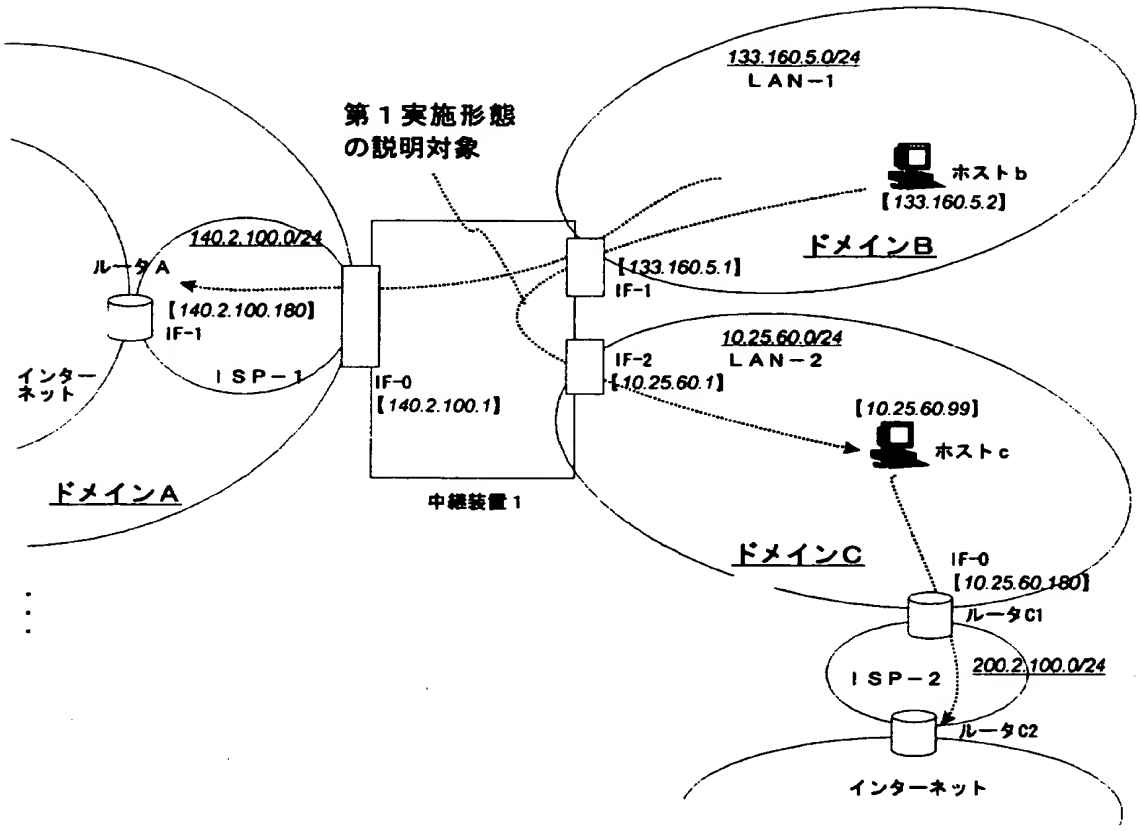
１３　　メモリ

１４　　ＣＰＵ

【書類名】　　図面

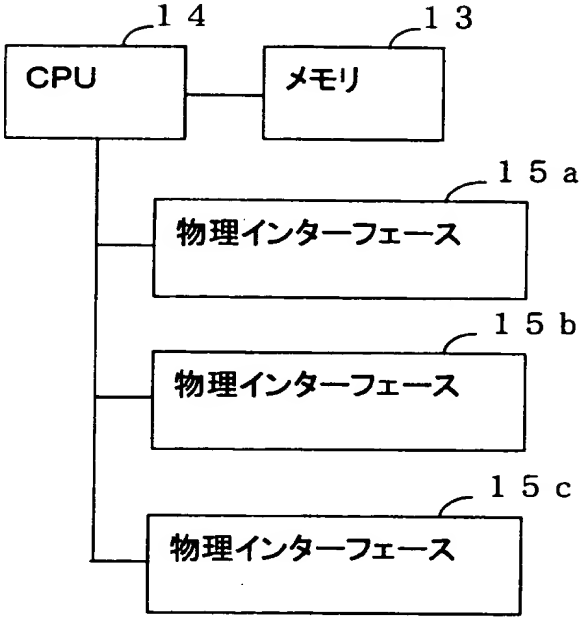
【図１】

第１実施形態のネットワーク構成図



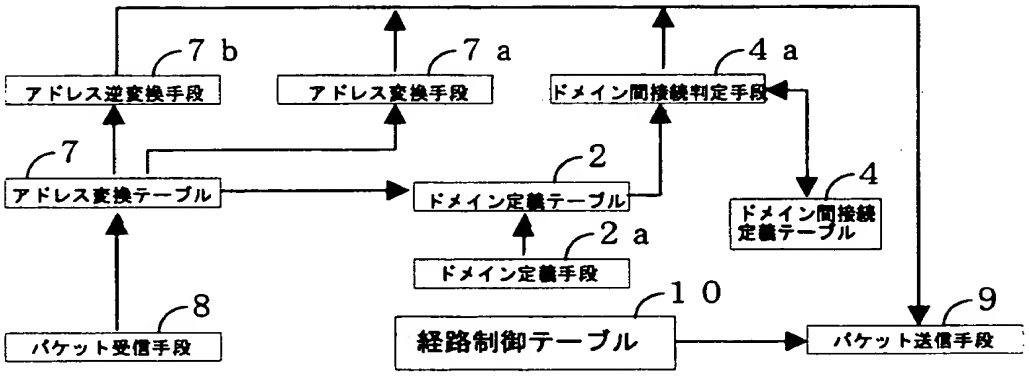
【図２】

通信装置１のハードウェア構成図



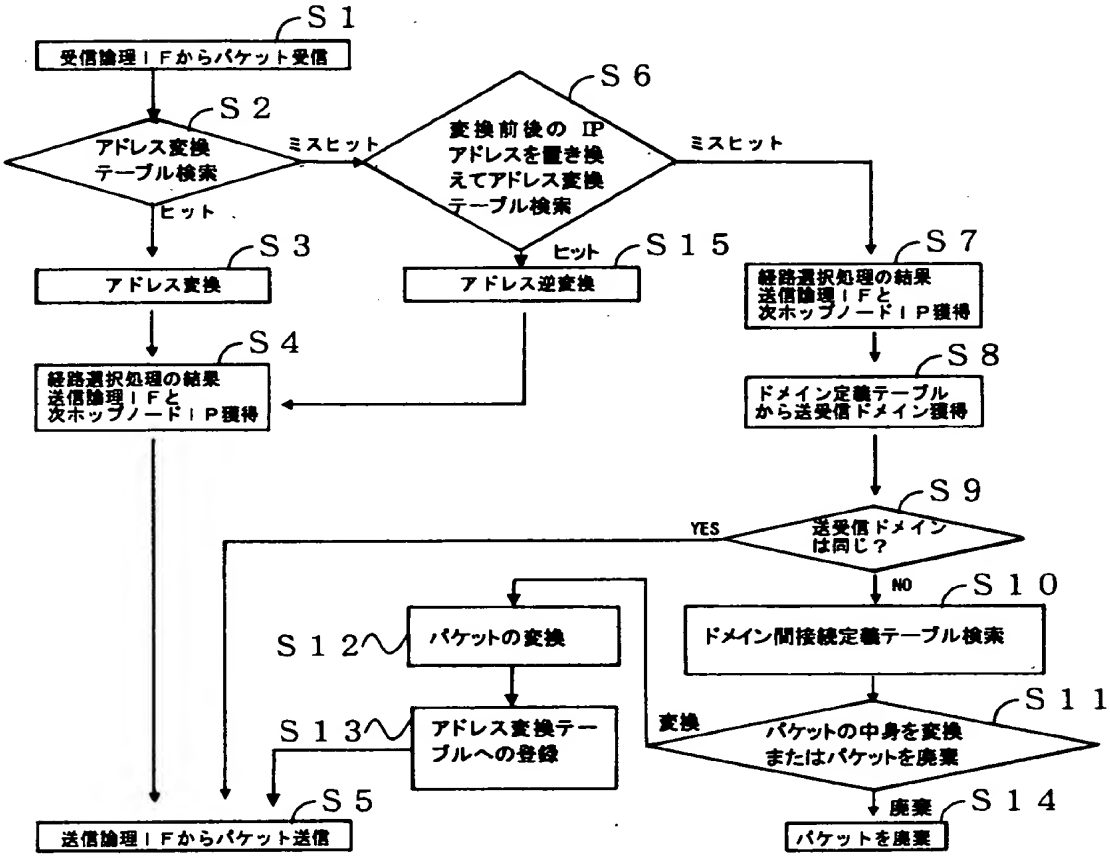
【図３】

第１実施形態における中継装置１の機能構成図



【図４】

第１実施形態における中継装置１の処理を示すフローチャート



【図５】

ドメイン定義テーブル２

論理インタフェース	ドメイン
IF-0	A
IF-1	B
IF-2	C

【図６】

ドメイン間接続定義テーブル４

受信ドメイン / 送信ドメイン	A	B	C
A	—	×	×
B	N	—	N
C	×	×	—

【図７】

アドレス変換テーブル７

変換前 IP アドレス	変換後 IP アドレス
133.160.5.2	10.25.60.2
・・・・・	・・・・・

【図８】

経路情報テーブル１０

宛先 IP アドレス	ネットマスク	次ホップノードの IP アドレス	送信論理インターフェース
140.2.100.0	255.255.255.0	—	IF-0
133.160.5.0	255.255.255.0	—	IF-1
10.25.60.0	255.255.255.0	—	IF-2
0.0.0.0	0.0.0.0	140.2.100.180	IF-0

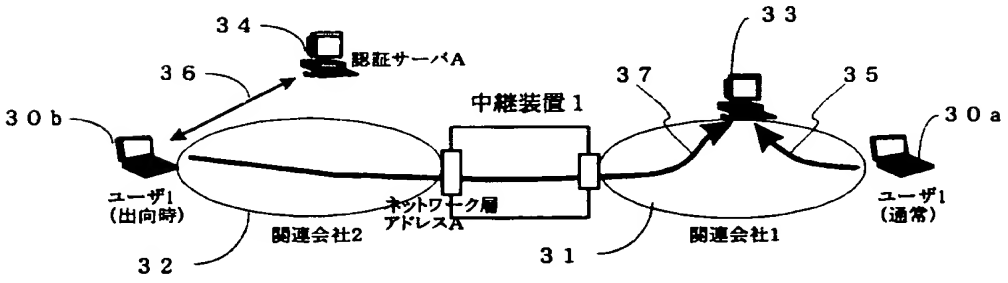
【図９】

第２実施形態におけるドメイン定義テーブル２

IP アドレス	ネットマスク	ドメイン
140.2.100.0	255.255.255.0	A
133.160.5.0	255.255.255.0	B
10.25.60.0	255.255.255.0	C
0.0.0.0	0.0.0.0	A

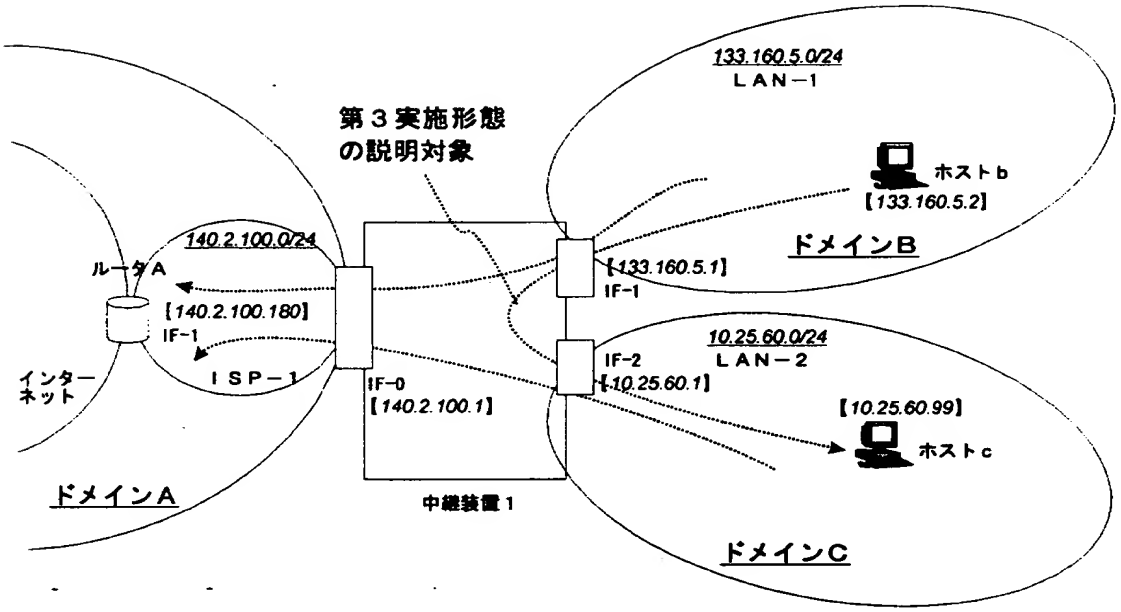
【図１０】

認証サーバと中継装置との組み合わせ



【図１１】

第３実施形態のネットワーク構成図



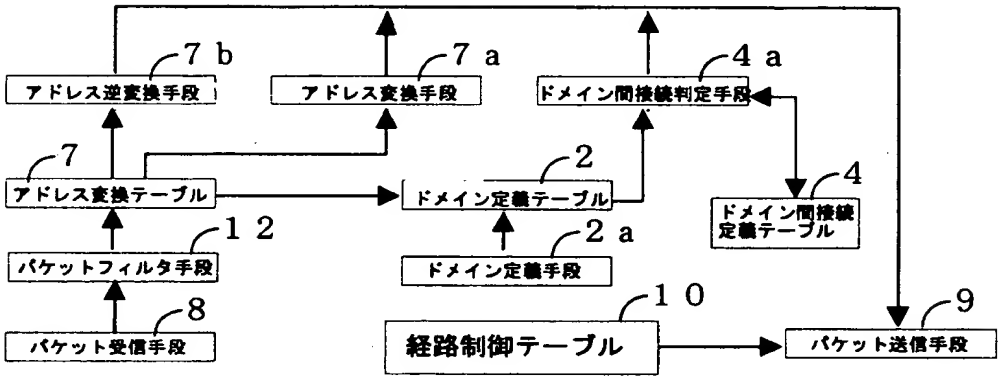
【図１２】

実施形態３におけるドメイン間接続定義テーブル４

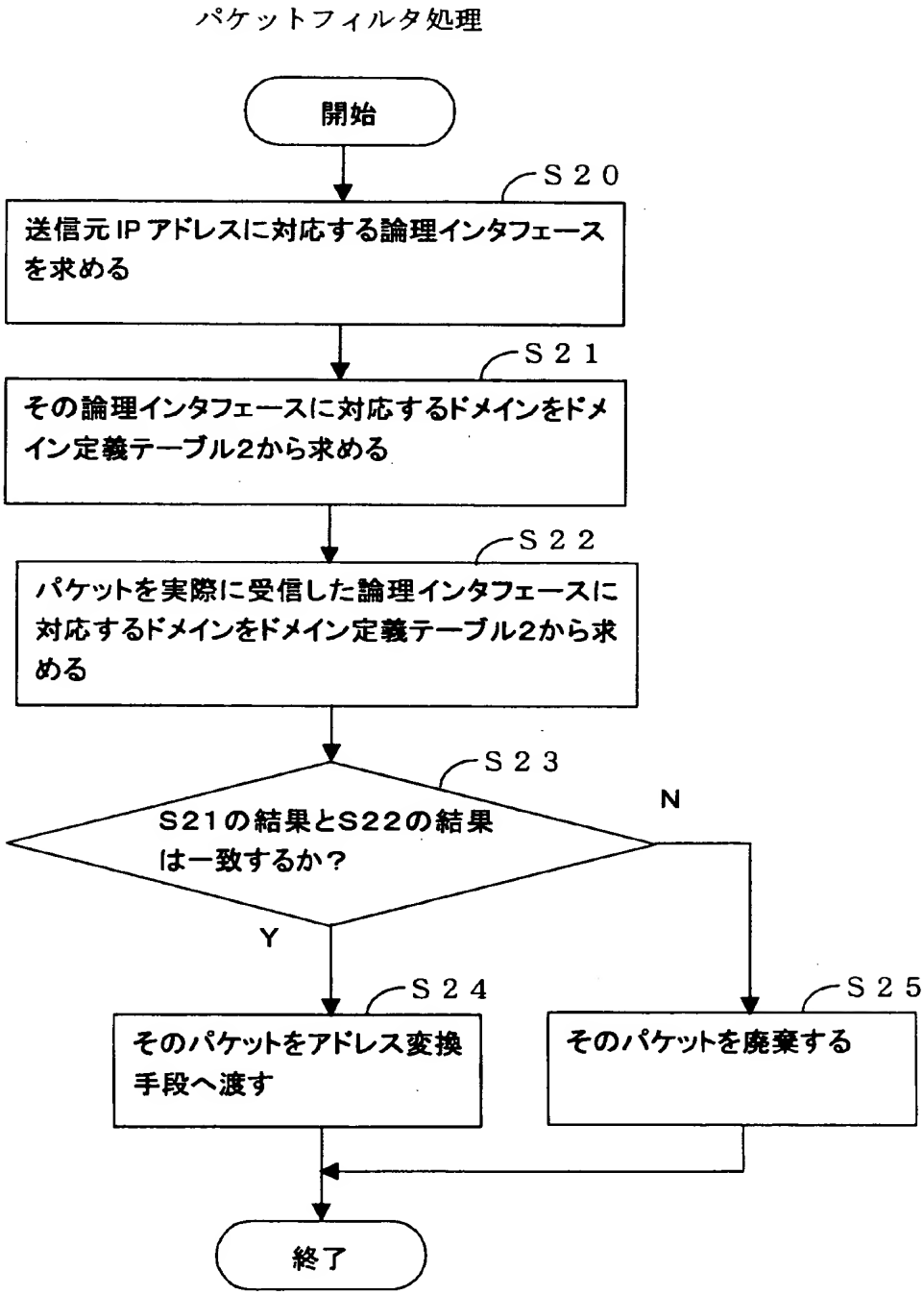
受信ドメイン / 送信ドメイン	A	B	C
A	—	×	×
B	N	—	N
C	N	×	—

【図１３】

第３実施形態における中継装置１の機能構成図



【図１４】


パケットフィルタ処理
開始
S２０
送信元IPアドレスに対応する論理インタフェースを求める
S２１
その論理インタフェースに対応するドメインをドメイン定義テーブル2から求める
S２２
パケットを実際に受信した論理インタフェースに対応するドメインをドメイン定義テーブル2から求める
S２３
S21の結果とS22の結果は一致するか？
N
Y
S２４
そのパケットをアドレス変換手段へ渡す
S２５
そのパケットを廃棄する
終了

【書類名】　要約書

【要約】

【課題】

本発明は、１以上のネットワークを接続したシステムとしてのドメインを定義・管理し、セキュリティや保守の独立性を確保した上で、ドメイン間を制限的に接続をすることを技術的課題とする。

【解決手段】

本発明は、各々１以上の通信装置を接続した、そのような２以上のネットワークを中継する通信データ中継装置であって、

ネットワークにアクセスするための２以上のインターフェース部と、

１以上のネットワークを接続したシステムとしてのドメインを定義するドメイン定義部と、

２以上のドメイン間における接続の可否を定義するドメイン間接続定義部と、

通信データの中継先を記憶する経路情報記憶部と、

異なるドメイン間で通信データを中継するときに、送信側ドメインにおける送信元アドレスと中継先ドメインにおける送信元アドレスとを相互に変換するアドレス変換部と、

ドメイン間接続定義部の定義に従い、２以上のドメイン間における中継の可否を制御する制御部とを備えたものである。

【選択図】　図１

出証特２０００－３１０４６９９

出　願　人　履　歴　情　報

識別番号　　〔０００００５２２３〕

１．変更年月日　　１９９６年　３月２６日
［変更理由］　住所変更
住　所　神奈川県川崎市中原区上小田中４丁目１番１号
氏　名　富士通株式会社